

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-277664

(43)Date of publication of application : 22.10.1996

(51)Int.Cl.

E05B 49/00

B60J 5/00

E05B 65/20

(21)Application number : 07-080079

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 05.04.1995

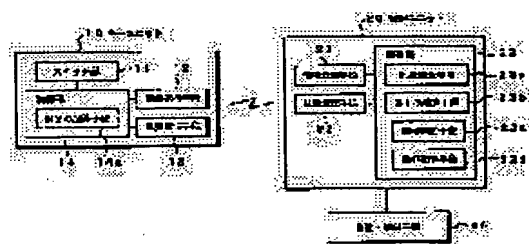
(72)Inventor : KISHI KAZUYA

(54) ELECTRONIC KEY SYSTEM

(57)Abstract:

PURPOSE: To provide an electronic key system having a very low possibility of being decoded by calculating coded functions based on authentication codes and random numbers at both a control unit and a key unit, and collating them.

CONSTITUTION: When the prescribed information is transmitted from a key unit 10, a control unit 20 generates a random number with a random number generating means 23a in response to it and sends it to the key unit 10. The control unit 20 also calculates the coded function with the first arithmetic means 23b based on the random number and the inherent authentication code. The key unit 10 calculates the coded function with the second arithmetic means 14a based on the received random number and the inherent authentication code and transmits it to the control unit 20. The control unit 20 collates both coded functions with a code judging means 23c, judges whether the prescribed conditions are satisfied or not, and controls a locking/unlocking means based on it for locking or unlocking.



LEGAL STATUS

[Date of request for examination] 22.02.2002

[Date of sending the examiner's decision of rejection] 06.09.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's]

decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平8-277664

(43)公開日 平成8年(1996)10月22日

(51)Int.Cl.⁶

E 0 5 B 49/00

B 6 0 J 5/00

E 0 5 B 65/20

識別記号

片内整理番号

F I

E 0 5 B 49/00

B 6 0 J 5/00

E 0 5 B 65/20

技術表示箇所

J

M

審査請求 未請求 請求項の数 2 O L (全 11 頁)

(21)出願番号

特願平7-80079

(71)出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(22)出願日

平成7年(1995)4月5日

(72)発明者 岸 和也

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

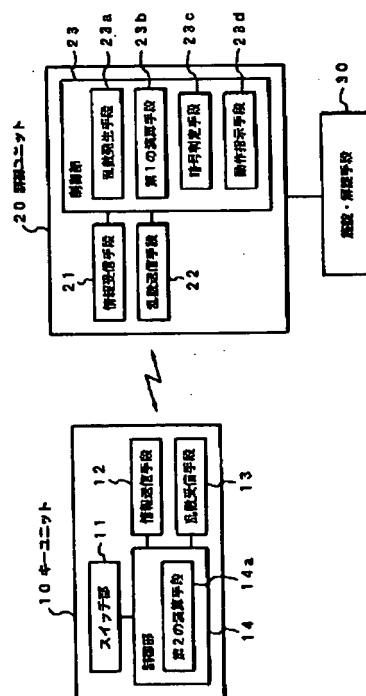
(74)代理人 弁理士 船橋 國則

(54)【発明の名称】 電子キーシステム

(57)【要約】

【目的】 本発明は、例えば赤外光や電波等を用いて施錠または解錠を行うもので、施錠または解錠を行う際に暗証コードが直接送受信されることのない電子キーシステムを提供することを目的とする。

【構成】 キーユニット10と制御ユニット20と施錠・解錠手段30とから構成され、前記キーユニット10及び前記制御ユニット20がそれぞれ固有の暗証コードを有する電子キーシステムにおいて、キーユニット10と制御ユニット20の間では、乱数と、その乱数及び前記暗証コードより演算された暗号化関数とが送受信されることにより互いの認証を行って、その結果施錠・解錠手段30で施錠または解錠が行われることを特徴とする。



第1実施例の電子キーシステムのブロック図

【特許請求の範囲】

【請求項1】 情報を送信する情報送信手段を備えたキーユニットと、

前記情報送信手段から送信された情報を受信する情報受信手段を備えた制御ユニットと、

該制御ユニットからの指示に従い施錠または解錠を行う施錠・解錠手段とから構成され、

前記キーユニットと前記制御ユニットとはそれぞれ固有の暗証コードを有している電子キーシステムにおいて、

前記制御ユニットには、前記情報送信手段からの所定の情報を前記情報受信手段で受信すると乱数を発生する乱数発生手段と、

該乱数発生手段が発生した乱数と前記制御ユニットに固有の暗証コードとを基に暗号化関数を演算する第1の演算手段と、

前記乱数発生手段が発生した乱数を前記キーユニットに送信する乱数送信手段とが設けられ、

前記キーユニットには、前記乱数送信手段から送信された乱数を受信する乱数受信手段と、

該乱数受信手段で受信した乱数と前記キーユニットに固有の暗証コードとを基に暗号化関数を演算する第2の演算手段とが設けられ、

さらに、前記制御ユニットには、前記第2の演算手段で演算された暗号化関数が前記情報送信手段から前記情報受信手段へ送信されると、送信された暗号化関数と前記第1の演算手段で演算された暗号化関数とが予め設定された所定の条件を満足するか否かを判定する暗号判定手段と、

該暗号判定手段が所定の条件を満足すると判定した場合に、前記施錠・解錠手段に施錠または解錠を行うように指示を与える動作指示手段とが設けられたことを特徴とする電子キーシステム。

【請求項2】 前記キーユニットには、該キーユニットに固有の暗証コードを記憶する第1の記憶手段が設けられ、

前記制御ユニットには、該制御ユニットに固有の暗証コードを記憶する第2の記憶手段が設けられ、

前記キーユニットと前記制御ユニットとの少なくとも一方に新たな暗証コードを送信する書き換え指示手段と、

前記暗号判定手段により前記第1の演算手段で演算された暗号化関数と前記第2の演算手段で演算された暗号化関数とが所定の条件を満足すると判定された後に、前記書き換え指示手段から前記新たな暗証コードが送信されると、前記第1の記憶手段に記憶されている暗証コードと前記第2の記憶手段に記憶されている暗証コードとの両方を前記新たな暗証コードに書き換える暗証コード書き換え手段とを備えてなることを特徴とする請求項1記載の電子キーシステム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、例えば赤外光や電波等を用いて施錠または解錠を行う電子キーシステムに関するものである。

【0002】

【従来の技術】 従来、電子キーシステムとしては、例えば自動車のドアに用いられているものが知られている。この電子キーシステムは、赤外光や電波等を介することによって、使用者が非接触で自動車のドアの施錠または解錠を行えるようにしたものであり、図5に示すように、使用者が携帯するキーユニット50と、自動車のドアに設けられている制御ユニット60と、ドアの施錠または解錠を行うソレノイド70とから構成されているものである。

【0003】 キーユニット50は、このキーユニット50に固有の暗証コードを、例えば予め回路上のパターンに刻み込まれたことによって有しているものであり、さらに、使用者が操作するためのスイッチ部51と、赤外光や電波等を介して前記暗証コードを送信する送信部52とを備えてなるものである。制御ユニット60は、キーユニット50と同様にこの制御ユニット60に固有な暗証コードを有しているものであり、さらに、受信部61と、判定部62と、動作指示部63とを備えてなるものである。受信部61は、キーユニット50の送信部52からの暗証コードを受信するものである。判定部62は、受信部61で受信した暗証コードと制御ユニット60が有している暗証コードとが一致するか否かを判定するものである。動作指示部63は、判定部62による判定結果に従い、ソレノイド70に対して動作指示を行うものである。

【0004】 このような電子キーシステムでは、使用者がキーユニット50のスイッチ部51を操作すると、送信部52がこのキーユニット50の有している暗証コードを赤外光や電波等を介して制御ユニット60へ送信する。キーユニット50から暗証コードが送信されると、制御ユニット60では、受信部61でその暗証コードを受信し、判定部62で受信した暗証コードとこの制御ユニット60の有している暗証コードとが一致するか否かを判定する。そして、判定部62によりそれぞれの暗証コードが一致すると判定されると、動作指示部63では、ソレノイド70に対して動作指示を与える。従って、キーユニット50に固有の暗証コードと制御ユニット60に固有の暗証コードとが一致すれば、ソレノイド70の動作によってドアの施錠または解錠が行われる。

【0005】

【発明が解決しようとする課題】 しかしながら、上述した電子キーシステムでは、キーユニット50と制御ユニット60の間で暗証コードが直接送受信されるようになっているため、第三者にその暗証コードが解読されてしまい、キーユニットが偽造される恐れがある。

【0006】 また、上述した電子キーシステムは、暗証

3

コードが同一であるキーユニット50及び制御ユニット60を一对とすると、他のキーユニットによる施錠または解錠を防ぐために、各対毎に異なる暗証コードを有していなければならない。但し、キーユニット50及び制御ユニット60には、予め暗証コードが回路上のパターン等に刻み込まれているので、例えば製造過程や保守交換時等においてはキーユニット50及び制御ユニット60を各対毎、即ち暗証コード毎に管理しなければならず、その管理が煩雑なものとなってしまう、製造過程や保守交換時等における作業効率の低下の一因となってしまう。そのために、例えばキーユニット50及び制御ユニット60の有している暗証コードを書き換え可能にすることが考えられるが、この場合に第三者であっても暗証コードの書き換えが可能であると、電子キーシステムとしての機能を果たさなくなってしまう。

【0007】そこで、本発明は、施錠または解錠を行う際に暗証コードが直接送受信されることのない電子キーシステムを提供することを目的とする。さらに、本発明は、第三者に暗証コードが書き換えられることなく、所望する暗証コードに書き換えることが可能な電子キーシステムを提供することを目的とする。

【0008】

【課題を解決するための手段】本発明は、上記目的を達成するために案出された電子キーシステムで、情報を送信する情報送信手段を備えたキーユニットと、前記送信手段から送信された情報を受信する情報受信手段を備えた制御ユニットと、この制御ユニットからの指示に従い施錠または解錠を行う施錠・解錠手段とから構成され、前記キーユニットと前記制御ユニットとはそれぞれ固有の暗証コードを有しているものであり、その上、前記制御ユニットには、前記情報送信手段からの所定の情報を前記情報受信手段で受信すると乱数を発生する乱数発生手段と、この乱数発生手段が発生した乱数と前記制御ユニットに固有の暗証コードとを基に暗号化関数を演算する第1の演算手段と、前記乱数発生手段が発生した乱数を前記キーユニットに送信する乱数送信手段とが設けられ、一方、前記キーユニットには、前記乱数送信手段から送信された乱数を受信する乱数受信手段と、この乱数受信手段で受信した乱数と前記キーユニットに固有の暗証コードとを基に暗号化関数を演算する第2の演算手段とが設けられ、さらに、前記制御ユニットには、前記第2の演算手段で演算された暗号化関数が前記情報送信手段から前記情報受信手段へ送信されると、送信された暗号化関数と前記第1の演算手段で演算された暗号化関数とが予め設定された所定の条件を満足するか否かを判定する暗号判定手段と、この暗号判定手段が所定の条件を満足すると判定した場合に、前記施錠・解錠手段に施錠または解錠を行うように指示を与える動作指示手段とが設けられたことを特徴とする。

【0009】また、前記キーユニットには、このキーユ

4

ニットに固有の暗証コードを記憶する第1の記憶手段が設けられ、前記制御ユニットには、この制御ユニットに固有の暗証コードを記憶する第2の記憶手段が設けられ、さらに、前記キーユニットと前記制御ユニットとの少なくとも一方に新たな暗証コードを送信する書き換え指示手段と、前記暗号判定手段により前記第1の演算手段で演算された暗号化関数と前記第2の演算手段で演算された暗号化関数とが所定の条件を満足すると判定された後に、前記書き換え指示手段から前記新たな暗証コードが送信されると、前記第1の記憶手段に記憶されている暗証コードと前記第2の記憶手段に記憶されている暗証コードとの両方を前記新たな暗証コードに書き換える暗証コード書き換え手段とを備えてなるものであってもよい。

【0010】

【作用】上記構成の電子キーシステムによれば、以下のような作用を奏する。まず、キーユニットの情報送信手段から所定の情報が送信されると、制御ユニットでは、情報受信手段でその情報を受信し、その情報に対応して乱数発生手段で乱数を発生して、その乱数を乱数送信手段でキーユニットへ送信する。これと同時に、制御ユニットでは、乱数発生手段で発生した乱数とこの制御ユニットに固有の暗証コードとを基に、第1の演算手段で暗号化関数を演算する。一方、キーユニットでは、制御ユニットの乱数送信手段から乱数が送信されると、乱数受信手段でその乱数を受信し、その乱数とこのキーユニットに固有の暗証コードとを基に第2の演算手段で暗号化関数を演算し、その暗号化関数を情報送信手段で制御ユニットへ送信する。そして、制御ユニットでは、キーユニットの情報送信手段からの暗号化関数を情報受信手段で受信すると、暗号判定手段によって受信した暗号化関数と第1の演算手段で演算した暗号化関数とが所定の条件を満足するか否かを判定する。このとき、第1の演算手段は、乱数発生手段が発生した乱数と制御ユニットに固有の暗証コードとを基に暗号化関数を演算し、また、第2の演算手段は、乱数発生手段が発生した乱数とキーユニットに固有の暗証コードとを基に暗号化関数を演算している。よって、例えば、制御ユニットに固有の暗証コードとキーユニットに固有の暗証コードとがそれぞれ同一であり、かつ、第1の演算手段と第2の演算手段とが同一の演算を行えば、前記第1の演算手段による暗号化関数と前記第2の演算手段による暗号化関数とは共に一致する。そして、暗号判定手段により判定される所定の条件が、例えば第1の演算手段による暗号化関数と第2の演算手段による暗号化関数とが共に一致することであれば、前記暗号判定手段では、それぞれの暗号化関数が所定の条件を満足すると判定する。暗号判定手段によりそれぞれの暗号化関数が所定の条件を満足すると判定された場合には、動作指示手段が施錠・解錠手段に施錠または解錠を行うように指示を与え、前記施錠・解錠手

段において施錠または解錠が行われる。

【0011】また、キーユニットに第1の記憶手段を設け、制御ユニットに第2の記憶手段を設け、さらに書き換え指示手段と暗証コード書き換え手段とを備えれば、以下のような作用を奏する。第1の記憶手段では、キーユニットに固有の暗証コードを記憶している。また、第2の記憶手段では、制御ユニットに固有の暗証コードを記憶している。ここで、暗号判定手段により第1の演算手段で演算された暗号化関数と第2の演算手段で演算された暗号化関数とが所定の条件を満足すると判定された後、書き換え指示手段から新たな暗証コードが送信されると、暗証コード書き換え手段では、第1の記憶手段に記憶されている暗証コードと第2の記憶手段に記憶されている暗証コードとの両方を前記新たな暗証コードに書き換える。従って、第1の記憶手段及び第2の記憶手段には、新たな暗証コードがそれぞれに固有な暗証コードとして記憶される。

【0012】

【実施例】以下、図面に基づき本発明に係わる電子キーシステムについて説明する。但し、ここでは、本発明を自動車のドアの施錠または解錠を行う電子キーシステムに適用した場合について説明する。

【0013】〔第1実施例〕本実施例の電子キーシステムは、請求項1記載の発明に係わる電子キーシステムであり、図1に示すように、キーユニット10と、制御ユニット20と、施錠・解錠手段30とを備えて構成されるものである。

【0014】キーユニット10は、使用者が携帯できるようにになっているもので、スイッチ部11と、情報送信手段12と、乱数受信手段13と、制御部14とを備えてなるものである。スイッチ部11は、押しボタンスイッチ等からなるもので、使用者が自動車のドアの施錠または解錠を行うためにONするものである。情報送信手段12は、赤外光や電波等を発信することにより、後述する情報を制御部14からの指示に従い、制御ユニット20へ送信するものである。乱数受信手段13は、後述する制御ユニット20の乱数送信手段22から乱数Rの格納されている情報が送信されると、その情報を受信するものである。

【0015】制御部14は、CPU (central processing unit) 等からなるもので、例えばこの制御部14の回路上のパターンに予めこのキーユニット10に固有な暗証コードK-codeを保持しているとともに、第2の演算手段14aを備えたものである。第2の演算手段14aは、乱数受信手段13で受信した情報から乱数Rを取り出して、この乱数Rとキーユニット10に固有な暗証コードK-codeとを基に、暗号化関数 $f(R, K-code)$ を演算するものである。また、この制御部14では、スイッチ部11がONされると“ASK(R)”というコマンドを、さらに第2の演算手段14aが暗号化関数 $f(R, K-code)$ を演

算すると、その暗号化関数 $f(R, K-code)$ を格納した“SEND($f(R, K-code)$)”というコマンドを、それぞれ制御ユニット20へ送信するように情報送信手段12に対して指示を与えるようになっている。

【0016】制御ユニット20は、自動車のドアに設けられているもので、情報受信手段21と、乱数送信手段22と、制御部23とを備えてなるものである。情報受信手段21は、キーユニット10の情報送信手段12からの情報、即ち“ASK(R)”というコマンドと“SEND($f(R, K-code)$)”というコマンドとを受信するものである。乱数送信手段22は、制御部23の指示に従い、後述する乱数発生手段23aが発生した乱数Rを“RETURN(R)”というコマンドに格納し、赤外光や電波等を用いてキーユニット10の乱数受信手段13へ送信するものである。

【0017】制御部23は、CPU等からなるもので、キーユニット10の制御部14と同様にこの制御ユニット20に固有な暗証コードK-codeを保持しているとともに、乱数発生手段23aと、第1の演算手段23bと、暗号判定手段23cと、動作指示手段23dとを備えてなるものである。但し、この制御部23では、キーユニット10の制御部14と同一の暗証コードK-codeを保持しているものとする。乱数発生手段23aは、情報受信手段21が情報送信手段12からの“ASK(R)”というコマンドを受信すると、乱数Rを発生するものである。第1の演算手段23bは、乱数発生手段23aが乱数Rを発生すると、その乱数Rと制御ユニット20に固有な暗証コードK-codeとを基に、暗号化関数 $f(R, K-code)$ を演算するものである。但し、この第1の演算手段23bでは、第2の演算手段14aと同じ暗号化関数 $f(R, K-code)$ を演算するようになっている。

【0018】暗号判定手段23cは、情報受信手段21が情報送信手段12からの“SEND($f(R, K-code)$)”というコマンドを受信すると、そのコマンドより第2の演算手段14aで演算された暗号化関数 $f(R, K-code)$ を取り出して、この暗号化関数 $f(R, K-code)$ と第1の演算手段23bで演算された暗号化関数 $f(R, K-code)$ とが予め設定されている所定の条件を満足するか否か、即ち、第1の演算手段23bによる暗号化関数 $f(R, K-code)$ と第2の演算手段14aによる暗号化関数 $f(R, K-code)$ とが一致するか否かを判定するものである。動作指示手段23dは、暗号判定手段23cにおいて第1の演算手段23bによる暗号化関数 $f(R, K-code)$ と、第2の演算手段14aによる暗号化関数 $f(R, K-code)$ とが一致すると判定されると、施錠・解錠手段30に対してドアの施錠または解錠を行うように指示を与えるものである。

【0019】施錠・解錠手段30は、ソレノイド等からなり、制御ユニット20と同様に自動車のドアに設けられ、かつその制御ユニット20と電気的に接続されているものである。また、制御ユニット20では、動作指示

7

手段23dからの指示に従って、例えば自動車のドアが施錠されていれば解錠を、また自動車のドアが解錠されていれば施錠を行うようになっている。

【0020】次に、以上のように構成された電子キーシステムにおいて、自動車のドアの施錠または解錠を行う動作例について、図2のフローチャートに従い説明する。キーユニット10では、赤外光や電波等が制御ユニット20に届く範囲内において使用者によりスイッチ部11がONされると(ステップ101、以下ステップをSと略す)、情報送信手段12が制御部14の指示に従い“ASK(R)”というコマンドを制御ユニット20へ送信する(S102)。情報送信手段12から“ASK(R)”というコマンドが送信されると、制御ユニット20では、情報受信手段21でそのコマンドを受信し(S103)、さらに乱数発生手段23aで乱数Rを発生させる(S104)。

【0021】乱数発生手段23aが乱数Rを発生させると、制御ユニット20では、乱数送信手段22がその乱数Rを格納した“RETURN(R)”というコマンドをキーユニット10へ送信し、かつ、第1の演算手段24が前記乱数Rとこの制御ユニット20に固有な暗証コードK-codeとを基に、暗号化関数 $f(R, K-code)$ の演算を行う(S105)。一方、キーユニット10では、乱数送信手段22から送信された“RETURN(R)”というコマンドを乱数受信手段13で受信すると(S106)、第2の演算手段14aが受信したコマンドから乱数Rを取り出し、その乱数Rとキーユニット10に固有な暗証コードK-codeとを基に、暗号化関数 $f(R, K-code)$ の演算を行う(S107)。

【0022】第2の演算手段14aで暗号化関数 $f(R, K-code)$ が演算されると、情報送信手段12では、この暗号化関数 $f(R, K-code)$ を格納した“SEND($f(R, K-code)$)”というコマンドを制御ユニット20へ送信する(S108)。情報送信手段12から“SEND($f(R, K-code)$)”というコマンドが送信されると、制御ユニット20では、そのコマンドを情報受信手段21で受信する(S109)。そして、暗号判定手段23cでは、“SEND($f(R, K-code)$)”というコマンドから第2の演算手段14aで演算された暗号化関数 $f(R, K-code)$ を取り出して、その暗号化関数 $f(R, K-code)$ と第1の演算手段23bで演算された暗号化関数 $f(R, K-code)$ とが一致するか否かを判定する(S110)。

【0023】このとき、第1の演算手段23bでは、乱数発生手段23aが発生した乱数Rと制御ユニット20に固有な暗証コードK-codeとを基に、暗号化関数 $f(R, K-code)$ の演算を行っている。また、第2の演算手段14aでは、乱数受信手段13で受信した乱数R、即ち乱数発生手段23aが発生した乱数Rとキーユニット10に固有な暗証コードK-codeとを基に、暗号化関数 $f(R, K-code)$ の演算を行っている。従って、制御ユニット20に

8

固有な暗証コードK-codeと、キーユニット10に固有な暗証コードK-codeとがそれぞれ同一であれば、第1の演算手段23bによる暗号化関数 $f(R, K-code)$ と、第2の演算手段14aによる暗号化関数 $f(R, K-code)$ とは共に一致する。

【0024】暗号判定手段23cで第1の演算手段23bによる暗号化関数 $f(R, K-code)$ と、第2の演算手段14aによる暗号化関数 $f(R, K-code)$ とが一致すると判定された場合、即ちキーユニット10と制御ユニット20との暗証コードK-codeが互いに同一である場合には、動作指示手段23dからの指示に従い、施錠・解錠手段30では、自動車のドアの施錠または解錠を行う(S111)。また、暗号判定手段23cで第1の演算手段23bによる暗号化関数 $f(R, K-code)$ と、第2の演算手段14aによる暗号化関数 $f(R, K-code)$ とが一致しない判定された場合には、キーユニット10と制御ユニット20との暗証コードK-codeが互いに異なるので、動作指示手段23dでは、施錠または解錠を行う指示を与えない。よって、施錠・解錠手段30では、自動車のドアの施錠または解錠を行わない。

【0025】このように本実施例の電子キーシステムでは、キーユニット10と制御ユニット20との間において、乱数発生手段23aが発生した乱数Rと、第2の演算手段14aが演算した暗号化関数 $f(R, K-code)$ とを送受信するようになっている。従って、キーユニット10と制御ユニット20との間で暗証コードK-codeが直接送受信されることがなく、さらに乱数R及び暗号化関数 $f(R, K-code)$ は送受信を行う度に異なった値となるので、第三者に暗証コードK-codeが解読されドアが解錠されてしまう可能性を極めて低くすることができる。

【0026】〔第2実施例〕次に、請求項2記載の発明に係わる電子キーシステムについて説明する。但し、上述した第1実施例と同一の構成要素については、同一の符号を与えてその説明を省略する。本実施例の電子キーシステムは、図3に示すように、キーユニット10aと、制御ユニット20aと、施錠・解錠手段30と、書き換え指示手段40とを備えて構成されるものである。

【0027】キーユニット10aは、上述した第1実施例に加えて、第1の記憶手段15が設けられたものである。第1の記憶手段15は、例えばEEPROM(Electrically Erasable Programmable Read-Only Memory)のような電氣的に書き込み及び読み出しが可能な不揮発性メモリからなるもので、キーユニット10aに固有な暗証コードを記憶するためのものである。従って、このキーユニット10aでは、第1実施例と異なり、暗証コードK-codeが制御部14に保持されているのではなく、第1の記憶手段15に記憶されるようになっている。

【0028】制御ユニット20aは、上述した第1実施例に加えて、第2の記憶手段24が設けられ、かつ、制御部23が暗証コード書き換え手段23eを備えている

ものである。第2の記憶手段24は、第1の記憶手段15と同様に不揮発性メモリからなるもので、制御ユニット20aに固有な暗証コードを記憶するためのものである。従って、この制御ユニット20aでは、キーユニット10aと同様に、暗証コードK-codeが制御部23に保持されているのではなく、第2の記憶手段24に記憶されるようになっている。

【0029】暗証コード書き換え手段23eは、暗号判定手段23cにおいて第1の演算手段23bによる暗号化関数 $f(R, K-code)$ と第2の演算手段14aによる暗号化関数 $f(R, K-code)$ とが互いに一致すると判定された後に、後述する書き換え指示手段40から新たな暗証コードK-code' が送信されると、第1の記憶手段15に記憶されている暗証コードK-codeと第2の記憶手段24に記憶されている暗証コードK-codeとの両方を新たな暗証コードK-code' に書き換えるものである。即ち、暗証コード書き換え手段23eでは、暗号判定手段23cでキーユニット10aと制御ユニット20aとの暗証コードK-codeが互いに一致すると判定された後、予めこの暗証コード書き換え手段23eに設定されている所定時間内に、後述する書き換え指示手段40からの“REWRITE(K-code')”というコマンドを情報受信手段21で受信すると、そのコマンドから新たな暗証コードK-code' を取り出して、第2の記憶手段24に記憶されている暗証コードK-codeを、新たな暗証コードK-code' に書き換えるようになっている。さらに、暗証コード書き換え手段23eでは、取り出した新たな暗証コードK-code' を“RETURN(K-code')”というコマンドに格納して、乱数送信手段22から乱数受信手段13へ送信し、キーユニット10aに対して第1の記憶手段15に記憶されている暗証コードK-codeを、新たな暗証コードK-code' に書き換えるように指示を与えるようになっている。尚、乱数送信手段22と乱数受信手段13との間では、乱数発生手段23aが発生した乱数Rに加え、“RETURN(K-code')”というコマンドが送受信されるようになっている。

【0030】書き換え指示手段40は、制御ユニット20aに赤外光や電波等が届く範囲内において用いられるもので、スイッチ部41と、情報送信手段42と、暗証コード格納部43と、制御部44とを備えてなるものである。スイッチ部41は、キーユニット10aのスイッチ部11と同様に構成されたものであり、また情報送信手段42は、キーユニット10aの情報送信手段12と同様に構成されたものである。暗証コード格納部43は、書き換えようとする新たな暗証コードK-code' を予め保持しているものであり、例えばキーユニット10aの第1の記憶手段15と同様に不揮発性メモリからなるものである。但し、暗証コード格納部43は、例えばキーボード等の外部装置に接続されて、この外部装置で設定された新たな暗証コードK-code' を受け取るように構成されたものであってもよい。

【0031】制御部44は、キーユニット10aの制御部14と同様にCPU等からなるものである。但し、この制御部44では、スイッチ部41が押圧されると、暗証コード格納部43に保持されている新たな暗証コードK-code' を、“REWRITE(K-code')”というコマンドに格納し、そのコマンドを制御ユニット20aへ送信するように情報送信手段42に対して指示を与えるようになっている。つまり、書き換え指示手段40は、上述した機能を有するものであれば、例えばキーユニット10aと同様に構成されたものであってもよい。また、書き換え指示手段40は、例えばキーユニット10aに上述した機能を追加したもの、即ちキーユニット10aと一体に構成されたものであってもよい。

【0032】次に、以上のように構成された電子キーシステムにおいて、暗証コードを書き換える動作例について、図4のフローチャートに従い説明する。但し、使用者がキーユニット10aのスイッチ部11をONするステップから、暗号判定手段23cにおいてキーユニット10aと制御ユニット20aとの暗証コードK-codeが互いに同一であるか否かを判定するステップまでは（図4におけるS201～S210）、第1実施例と同様であるのでその説明を省略する。また、本実施例における施錠または解錠を行う動作例は、第1実施例と同様であるのでその説明を省略する。尚、キーユニット10aの第1の記憶手段15と制御ユニット20aの第2の記憶手段24には、予め同一の暗証コードK-codeが記憶されているものとする。

【0033】暗号判定手段23cで暗証コードK-codeが互いに同一であると判定されると、続いて使用者は、書き換え指示手段40のスイッチ部41をONする（S211）。但し、暗号判定手段23cで暗証コードK-codeが互いに同一でないと判定されると、暗証コードK-codeが同一でないキーユニット10a及び制御ユニット20aは、暗証コードK-codeを書き換える条件を満たしていないので、使用者がスイッチ部41をONしても書き換え動作は行われなない。スイッチ部41がONされると、書き換え指示手段40の情報送信手段42は、制御部44の指示に従って、新たな暗証コードK-code' を格納した“REWRITE(K-code')”というコマンドを制御ユニット20aへ送信する（S212）。

【0034】情報送信手段42から“REWRITE(K-code')”というコマンドが送信されると、制御ユニット20aでは、情報受信手段21でそのコマンドを受信する（S213）。そして、暗証コード書き換え手段23eでは、暗号判定手段23cで暗証コードK-codeが互いに同一であると判定されてから、情報受信手段21で“REWRITE(K-code')”というコマンドを受信するまでの時間が、この暗証コード書き換え手段23eに設定されている所定時間内であるか否かを判定する（S214）。即ち、暗証コード書き換え手段23eでは、使用者がキー

ユニット10aのスイッチ部11をONしてから、所定時間内に書き換え指示手段40のスイッチ部41をONしたか否かを判定する。

【0035】使用者が所定時間内にスイッチ部41をONしなかった場合には、暗証コード書き換え手段23eにより暗証コードK-codeを書き換える条件が満たされていないと判断され、書き替え動作は行われない。また、使用者が所定時間内にスイッチ部41をONした場合には、暗証コード書き換え手段23eでは、情報受信手段21で受信した“REWRITE(K-code)”というコマンドから新たな暗証コードK-code'を取り出して、その暗証コードK-code'を第2の記憶手段24に書き込む(S215)。これと同時に、暗証コード書き換え手段23eでは、取り出した暗証コードK-code'を“RETURN(K-code')”というコマンドに格納して乱数送信手段22へ送出する。そして、乱数送信手段22では、“RETURN(K-code')”というコマンドをキーユニット10aへ送信する(S216)。

【0036】乱数送信手段22から“RETURN(K-code')”というコマンドが送信されると、キーユニット10aでは、乱数受信手段13でそのコマンドを受信する(S217)。乱数受信手段13が“RETURN(K-code')”というコマンドを受信すると、制御部14では、そのコマンドから新たな暗証コードK-code'を取り出して、その暗証コードK-code'を第1の記憶手段15に書き込む(S218)。従って、第1の記憶手段15及び第2の記憶手段24には、共に新たな暗証コードK-code'が、それぞれに固有な暗証コードとして記憶される。

【0037】このように本実施例の電子キーシステムでは、キーユニット10aに固有な暗証コードK-codeが第1の記憶手段15に記憶され、また制御ユニット20aに固有な暗証コードK-codeが第2の記憶手段24に記憶され、これらの暗証コードK-codeが書き換え指示手段40からの指示に従い、暗証コード書き換え手段23eによって書き換えられるようになっている。従って、例えば製造過程において、予め全てのキーユニット10a及び制御ユニット20aに同一の暗証コードK-codeを記憶させ、出荷時に対となるキーユニット10a及び制御ユニット20aに新たな暗証コードK-code'を個別に記憶させるといったことが可能となるので、キーユニット10a及び制御ユニット20aを各対毎に管理する必要がなくなり、結果として管理の煩雑さを低減することができる。

【0038】また、本実施例の電子キーシステムでは、自動車のドアに搭載した後でも暗証コードK-codeの書き換えが行えるので、例えばキーユニット10aと制御ユニット20aとのいずれか一方に不具合が発生しても、キーユニット10aと制御ユニット20aとを一对として交換することなく、いずれか一方の交換及び暗証コー

ドK-codeの書き換えにより対応することができ、保守交換時における柔軟な対応が可能となる。つまり、本実施例の電子キーシステムでは、暗証コードK-codeの管理の煩雑さを低減することにより、製造過程や保守交換時等における作業効率の向上を図ることができる。

【0039】さらに、本実施例の電子キーシステムでは、暗号判定手段23cにおいてキーユニット10aと制御ユニット20aとの暗証コードK-codeが互いに同一であると判定された後に、書き換え指示手段40からの指示があれば、暗証コード書き換え手段23eが新たな暗証コードK-code'への書き換えを行うようになっている。従って、キーユニット10a及び制御ユニット20aが互いに同一である暗証コードK-codeを既に有している場合のみ、新たな暗証コードK-code'への書き換えが行われるので、第三者に暗証コードK-codeが書き換えられてしまう可能性が極めて低くなる。

【0040】尚、上述した第1実施例及び第2実施例では、本発明を自動車のドアに適用した場合について説明したが、本発明はこれに限定されるものではなく、例えば家屋のドアやロッカーの扉等にも適用可能である。また、上述した第1実施例及び第2実施例では、第1の演算手段23b及び第2の演算手段14aが同一の暗号化関数 $f(R, K-code)$ を演算し、かつ暗号判定手段23cでそれぞれの演算結果が一致するかどうかを判定する場合について説明したが、例えば第1の演算手段23bと第2の演算手段14aとで異なる暗号化関数 $f(R, K-code)$ を演算し、かつそれぞれの暗号化関数 $f(R, K-code)$ が所定の条件として予め暗号判定手段23cに設定され、この暗号判定手段23cによってそれぞれの演算結果が予め設定されている所定の条件を満足するかどうか判定される場合であってもよい。さらに、上述した第2実施例では、暗証コード書き換え手段23eを制御ユニット20aの制御部23に設けた場合について説明したが、例えば暗証コード書き換え手段23eをキーユニット10aの制御部14に設けてもよい。

【0041】

【発明の効果】以上に説明したように、本発明の電子キーシステムは、キーユニットと制御ユニットとの間において、乱数発生手段が発生した乱数と第2の演算手段が演算した暗号化関数とを送受信するようになっている。従って、キーユニットと制御ユニットとの間で暗証コードが直接送受信されることがなく、さらに乱数及び暗号化関数は送受信を行う度に異なった値となるので、第三者に暗証コードが解読される可能性が極めて低くなり、暗証コードの解読による施錠または解錠を防ぐことができるという効果を奏する。

【0042】また、キーユニットに第1の記憶手段を、制御ユニットに第2の記憶手段をそれぞれ設け、さらに書き換え指示手段と暗証コード書き換え手段とを備えれば、暗号判定手段が所定の条件を満足すると判定し、か

13

つ書き換え指示手段からの指示があった場合に、暗証コード書き換え手段によって暗証コードが書き換えられるようになっている。従って、キーユニット及び制御ユニットの暗証コードの書き換えが可能となるので、キーユニット及び制御ユニットを各対毎に管理する必要がなくなり、結果として管理の煩雑さを低減することが可能となり、例えば製造過程や保守交換時等における作業効率の向上を図ることができる。但し、キーユニット及び制御ユニットでは、暗号判定手段が所定の条件を満足すると判定した場合にのみ新たな暗証コードへの書き換えが行われるので、第三者に書き換えられてしまう可能性を極めて低くした上での暗証コードの書き換えを実現することができる。

【図面の簡単な説明】

【図1】本発明に係わる電子キーシステムの第1実施例の概略構成を示すブロック図である。

【図2】図1の電子キーシステムにおける施錠または解錠の動作例を示すフローチャートである。

【図3】本発明に係わる電子キーシステムの第2実施例の概略構成を示すブロック図である。

【図4】図3の電子キーシステムにおける暗証コードの

14

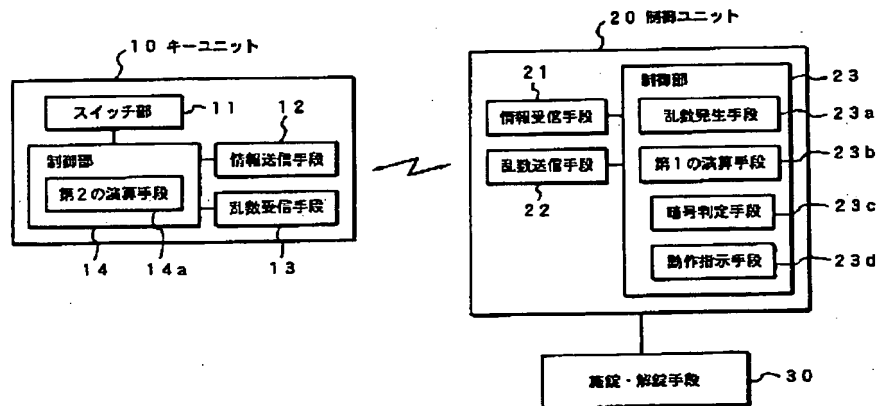
書き換えの動作例を示すフローチャートである。

【図5】従来例の電子キーシステムの概略構成を示すブロック図である。

【符号の説明】

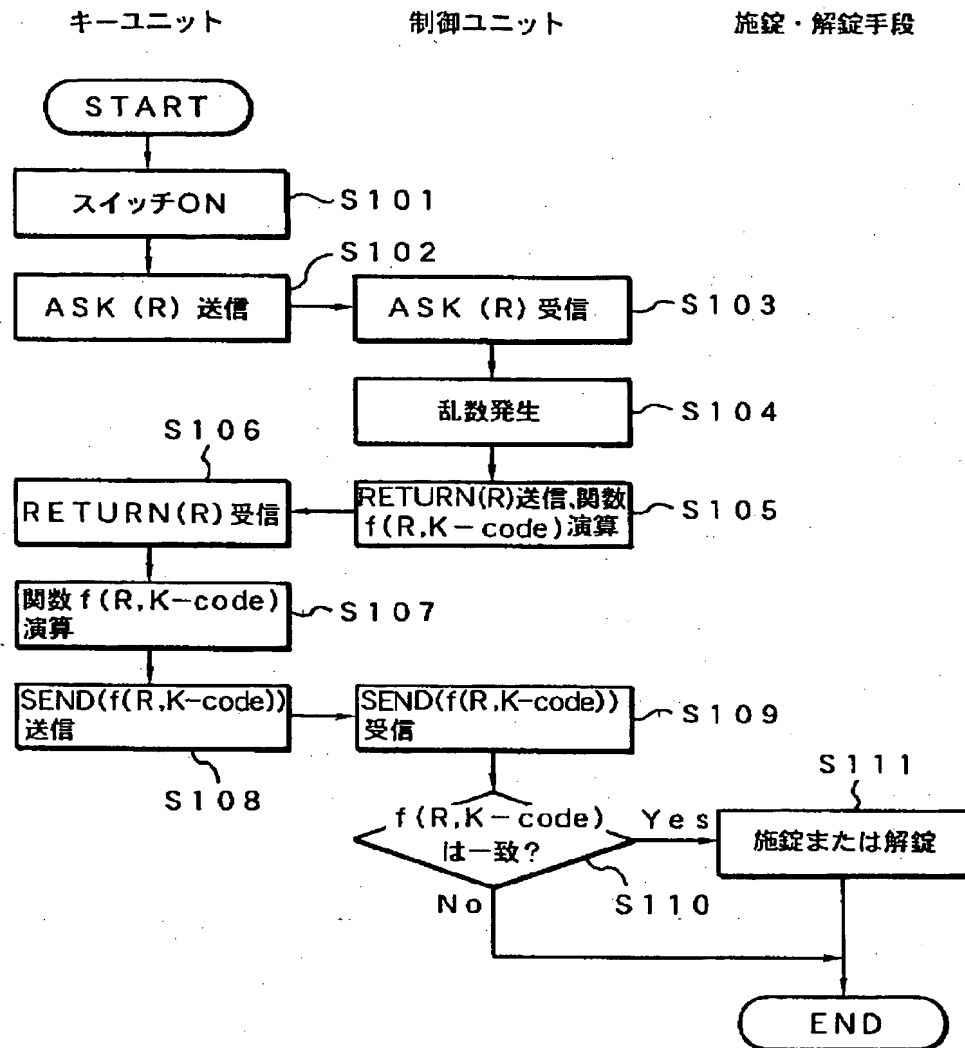
10、10a	キーユニット	12	情報送信手段
13	乱数受信手段	14a	第2の演算手段
15	第1の記憶手段	20、20a	制御ユニット
21	情報受信手段	22	乱数送信手段
23a	乱数発生手段	23b	第1の演算手段
23c	暗号判定手段	23d	動作指示手段
23e	暗証コード書き換え手段	24	第2の記憶手段
30	施錠・解錠手段	40	書き換え指示手段

【図1】



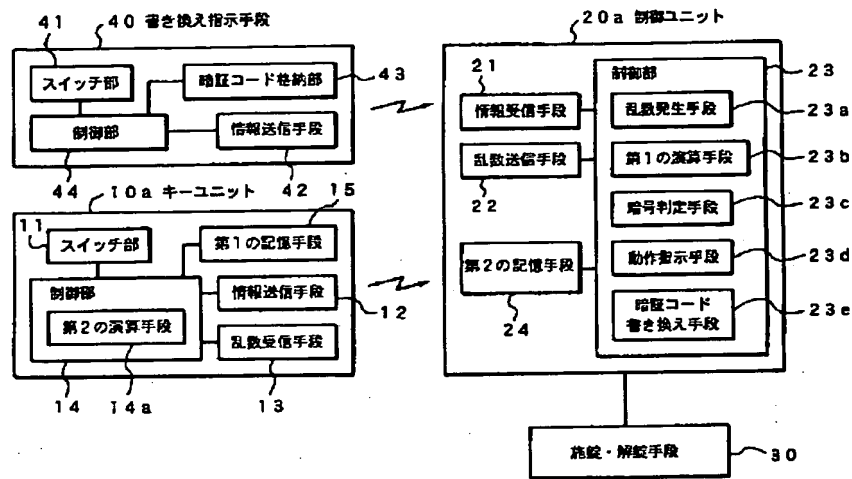
第1実施例の概略構成のブロック図

【図2】



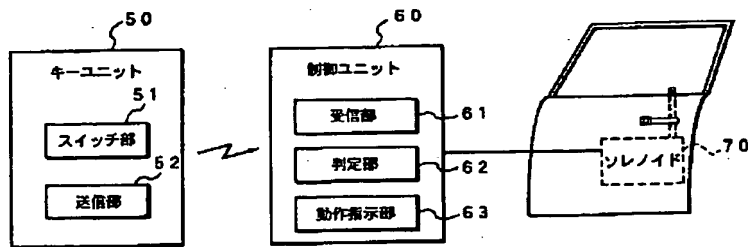
施錠／解錠の動作例のフローチャート

【図3】



第2実施例の概略構成のブロック図

【図5】



従来例の概略構成のブロック図

【図4】

